This listing of claims will replace all prior versions and listings of the claims in the application:

LISTING OF THE CLAIMS:

1. (Original) A method for verifying an electronic item, the method including:

(a) presenting a secure credential, the credential comprising predefined plural subsets of the electronic item and corresponding cryptographic hashes; and

(b) randomly selecting one of the predefined plural subsets;

(c) computing a cryptographic hash of a portion of the electronic item corresponding to the selected predefined subset; and

(d) testing whether the computed cryptographic hash corresponds to a corresponding cryptographic hash within the presented credential.

2. (Original) A method as in claim 1, including performing steps (b)-(d) multiple times.

3. (Original) A method as in claim 1, further including:

randomly selecting a second portion of the electronic item that does not correspond to one of the predefined plural subsets; and

requiring computation of a cryptographic hash of said second portion of the electronic item.

4. (Original) A method as in claim 1, wherein step (c) includes challenging the electronic item to compute said cryptographic hash.

5. (Original) A method as in claim 1, wherein step (c) includes accessing the electronic item via shared memory.

6. (Original) A method as in claim 1, wherein steps (b) and (c) are performed during execution of the electronic item.

7. (Currently Amended) In a computer system including an insecure arrangement for using an application[,] and a trusted element for verifying the application, the trusted element comprising:

a decryptor that decrypts a credential associated with the application;

a validator that validates at least one digital signature corresponding to the credential;

a challenge generator that selects, based at least in part on the credential, at least one predetermined portion of the application, and issues a challenge requesting a response from the insecure arrangement, the response providing a computation of at least one value based on the selected predetermined portion of the application; and

a response checker that checks the response against the credential.

8. (Original) A trusted element as in claim 7, wherein the challenge generator randomly selects the predetermined portion from plural predetermined portions defined by the credential.

9. (Original) A trusted element as in claim 7, wherein the challenge generator issues the challenge during execution of the application by the insecure computing arrangement.

10. (Original) A trusted element as in claim 7, wherein the challenge generator issues the challenge to the application to compute the value.

11. (Original) A trusted element as in claim 7, wherein the challenge generator requests the application to compute a cryptographic hash of the selected predetermined portion.

12. (Original) A trusted element as in claim 7, wherein the challenge generator selects a virtual path within the application.

13. (Original) A trusted element as in claim 7, wherein the challenge generator selects a byte range within the application.

14. (Original) A method for certifying an electronic item comprising:

(a) randomly selecting plural portions of the electronic item;

(b) computing at least one cryptographic value corresponding to each of the selected plural portions; and

(c) specifying a credential defining each of the randomly selected plural portions and the corresponding computed cryptographic values.

15. (Original) A method as in claim 14, wherein computing step (b) comprises computing a cryptographic hash value corresponding to each of the selected plural portions.

16. (Original) A method as in claim 14, wherein selecting step (a) comprises randomly selecting plural byte ranges within the electronic item.

17. (Original) A method as in claim 14, wherein selecting step (a) comprises randomly selecting plural virtual paths within the electronic item.

18. (Original) A method as in claim 14, further including the step of digitally signing the credential.

19. (Original) A method as in claim 14, further including the step of encrypting the credential.

20. (Original) A device for certifying an electronic item comprising:

means for randomly selecting plural portions of the electronic item;

means for computing at least one cryptographic value corresponding to each of the selected plural portions; and

means for specifying a credential defining at least one randomly-selected portion and the corresponding computed cryptographic value.

21. (Original) A device for certifying an electronic item comprising:

a selector that randomly selecting plural portions of the electronic item;

a computer that computes at least one cryptographic value corresponding to each of the selected plural portions; and

a credential formatter that formats one or more credentials defining at least one randomly-selected portion and the corresponding computed cryptographic value.

22. (Original) A device as in claim 21, wherein the computer computes a cryptographic hash value corresponding to each of the selected plural portions.

23. (Original) A device as in claim 21, wherein the selector randomly selects plural byte ranges within the electronic item.

24. (Original) A device as in claim 21, wherein the selector randomly selects plural virtual paths within the electronic item.

25. (Original) A device as in claim 21, further including a digital signer that digitally signs the one or more credentials.

26. (Original) A device as in claim 21, further including an encryptor that encrypts the one or more credentials.

27. (Canceled)